Abstract

Risk management methodologies, such as Mehari, Ebios, CRAMM and SP 800-30 (NIST) use a common step based on threat, vulnerability and probability which are typically evaluated intuitively using verbal hazard scales such as low, medium, high. Because of their subjectivity, these categories are extremely difficult to assign to threats, vulnerabilities and probability, or indeed, to interpret with any degree of confidence. The purpose of the paper is to propose a mathematical formulation of risk by using a lower level of granularity of its elements: threat, probability, criteria used to determine an asset’s value, exposure, frequency and existing protection measure.
REFERENCES


INDEX TERMS

Computer Science Security
Keywords
ISO27005  MEHARI  EBIOS  SP800-30 (Nist)  CRAMM.